DEGREE PROJECT IN TECHNOLOGY,
FIRST CYCLE, 15 CREDITS
STOCKHOLM, SWEDEN 2017

Are Cryptocurrencies the Future of Money?

Whether a Transition to Cryptocurrency, as National Currency of Sweden, Would be Possible and What it Would Imply for the Swedish Society

MADELEINE GARTZ

IDA LINDERBRANDT

KTH ROYAL INSTITUTE OF TECHNOLOGY
SCHOOL OF COMPUTER SCIENCE AND COMMUNICATION

Abstract

The underlying technology of cryptocurrencies is a broadly discussed subject. In Sweden, a growing interest for digital assets and payment methods can be observed. The fact that this coincides with an increasing acceptance for cryptocurrencies creates interesting possibilities. Some claim that cryptocurrency could be the future mean of payment. The objective of this report is therefore to examine whether a cryptocurrency could replace the Swedish krona, and what such a transition would imply for the Swedish society. To deliver a thorough analysis, the delimitation to exemplify with the cryptocurrency bitcoin and its protocol was made. Primarily, a literature study was conducted to determine the protocol's structure, security and usability, as well as its possibility to fulfil the functions of the Swedish krona. In addition, an interview with Björn Segendorf at the Riksbank was held, in order to obtain the Riksbank's interest and standpoint in the questions of matter.

A transition to cryptocurrency is associated with both advantages and disadvantages. The infrastructure behind Bitcoin creates a possibility to process certain payments more time and cost efficiently, and simultaneously provides open and decentralized participation as well as increased payer integrity. However, the Bitcoin protocol has limitations that should be considered and dealt with before a transition should be initialized. The large energy consumption required to process transactions could be considered the largest obstacle for Bitcoin's further growth. There are also security concerns, that could affect users of the protocol, that should be considered.

Sweden fulfils the technical prerequisites for Bitcoin, and any other cryptocurrency with similar structure. However, a cryptocurrency does not fulfil the functions of a traditional currency. A transition to cryptocurrency would also affect the Riksbank's possibility to conduct monetary policies. Following, the report concludes that a complete transition to cryptocurrency in Sweden seems unfavourable as of today. Cryptocurrencies are likely to grow continuously, and gain new market shares, but will coexist with traditional currencies and payment systems. It is not unlikely that a transition to cryptocurrency will occur in the future, when the market has matured, and solutions to problems highlighted in this report have been presented.

Sammanfattning

Tekniken bakom kryptovalutor har blivit ett hett diskuterat ämne. I Sverige urskiljs ett allt mer växande intresse för digitala tillgångar och betalmetoder, och att detta sammanfaller med en ökande acceptans för kryptovalutor skapar intressanta möjligheter. Vissa menar att kryptovaluta kan vara framtidens betalmedel. Rapportens frågeställning avhandlar därför huruvida en kryptovaluta skulle kunna ersätta den svenska kronan och vad det skulle innebära för det svenska samhället. För att utreda frågan har en avgränsning gjorts till att exemplifiera med kryptovalutan bitcoin och dess protokoll. Primärt har en litteraturstudie utförts kring såväl protokollets uppbyggnad och säkerhet som dess användarvänlighet och möjlighet att axla den svenska kronans funktioner. Dessutom har en intervju genomförts med Björn Segendorf på Riksbanken i syfte att ta del av Riksbankens intresse och ställningstagande i frågan.

Det finns såväl fördelar som nackdelar med en övergång till kryptovaluta. Infrastrukturen bakom bitcoin skapar möjlighet att tids- och kostnadseffektivisera betalningar inom vissa områden, och erbjuder samtidigt ett öppet, decentraliserat deltagande, samt ökad användarintegritet. Protokollet har dock begränsningar som bör tas i beaktande innan en övergång kan ske. Den höga energikonsumtion som krävs för att bearbeta transaktioner kan anses utgöra störst hinder för Bitcoins fortsatta framväxt. Dessutom finns flera säkerhetsaspekter som riskerar påverka användare av valutan negativt.

Sverige har tekniska förutsättningar för att övergå till en kryptovaluta med tekniska krav liknande de för Bitcoin. Emellertid kan en kryptovaluta inte anses uppfylla de krav som ställs på en valuta. En övergång till kryptovaluta skulle även påverka Riksbankens möjlighet att bedriva penningpolitik. Slutsatsen blir således att en total övergång till kryptovaluta i Sverige ter sig ogynnsam med dagens förutsättningar. Kryptovaluta kommer med största sannolikhet att fortsätta växa och ta marknadsandelar, men kommer att samexistera med traditionella valutor och betalningssystem. Det känns inte osannolikt att en övergång till kryptovaluta kommer att ske i framtiden när marknaden mognat och lösningar, på i rapporten belysta problem, presenterats.

Glossary

Bitcoin	The technical infrastructure of the cryptocurrency, also mentioned by the Bitcoin protocol
bitcoin	The cryptocurrency, units of value being transferred by the technical infrastructure Bitcoin
Satoshi	Satoshi Nakamoto, the anonymous creator of Bitcoin
satoshi	The smallest unit of value of Bitcoin, one hundred millionth fraction of a bitcoin
Address	Bitcoin identity, corresponding to account number in the traditional payment system
Wallet	A software used to store the access to one's funds in cryptocurrencies, for example bitcoin
Blockchain	A data structure that serves as a public ledger of all bitcoin transactions ever executed
Block height	A number indicating a block's position on the blockchain, used to identify a block
Node	Any computer that runs Bitcoin client software, participating in the peer-to-peer network that constitutes Bitcoin, by broadcasting transactions and blocks
Miner	A specialized node creating valid Bitcoin blocks, containing bitcoin transactions, that are put on the blockchain
Proof-of-Work	The consensus algorithm of Bitcoin, other cryptocurrencies have other consensus mechanisms
Hash puzzle	A problem, relying on both the random and deterministic properties of hashes, solved to prove Proof-of-Work

Table of Contents

1 Introduction

1.1 Background

In October 2008, the white paper "Bitcoin: A Peer-to-Peer Electronic Cash System" was published under the alias Satoshi Nakamoto. The paper described the ground-breaking idea of a cryptocurrency, solving the problem of double spending as well as eliminating the need of a central authority, for example a central bank, for money supply and security enforcing. Instead, the rules of the system are encoded within the system itself [1]. While the real identity of the system's creator remains unknown, his innovation, the Bitcoin protocol, has gained global recognition and laid the ground for a new market of cryptocurrencies.

A cryptocurrency is a digital asset intended to work as a medium of exchange using cryptography to secure the transaction. Bitcoin was the first cryptocurrency to be implemented but as of April 29th 2017, there exists over 800 cryptocurrencies with a total market capitalization of approximately 309BSEK. Today, Bitcoin dominates 61.4% of the cryptocurrency market and is subsequently followed by Ethereum, Ripple and Litecoin. [2]

The value of a cryptocurrency is created by the user, accepting it as a mean of payment. Cryptocurrencies rely on mathematics and encryption, in difference to traditional fiat currencies, which rely on central banks. Trust and adoption are what gives a currency its value, together with the user's anticipation of being able to use the currency in the future. Users of cryptocurrency are placing trust in the underlying structure rather than a central issuer. [3]

The cryptocurrency market creates new possibilities in numerous areas, since most cryptocurrencies provide both a payment infrastructure and a currency. This new technology, and especially the Bitcoin protocol, has caught the attention of the business sector and significant resources are being devoted to research within this area. Some claim that this new technology is the future of money and that it will change the payment systems of today [4].

In Sweden, a paradigm shift in payment methods can be observed. According to VISA, Sweden is the second most frequent user of card payments in Europe [5]. Simultaneously, the total value of Swedish coins and notes in circulation, 58BSEK, only constitutes a couple of percent of Sweden's total monetary supply [6]. In 2016, Sweden's e-commerce increased with 16% in terms of retail, and 31% in terms of food [7]. The fact that the increasing use of digital assets and payment methods coincides with the emerge of cryptocurrencies creates interesting possibilities. Could a cryptocurrency be the next step in Sweden's technical and financial development?

1.2 Purpose

The purpose of this report is to explore whether a transition to a cryptocurrency, exemplified with bitcoin, is possible and what opportunities and limitations it would imply. Since cryptocurrencies are broadly discussed, not least by the Riksbank who are currently investigating the possibility of implementing an e-krona [8], the subject is of contemporary relevance. This report is of interest not only to the Riksbank but also to financial institutes, individuals and businesses, who are curious of what a transition to a cryptocurrency would imply. The report will be based on Sweden's existing conditions regarding technology, acceptance and security and readers of this report are expected to have a basic understanding of technology and computer science.

1.3 Scientific Questions

Based on the presented background and purpose of this report, the following main objective has been defined:

Would a transition to a cryptocurrency, as national currency of Sweden, be possible and what would it imply for the Swedish society?

In order to determine this, four scientific questions have been specified:

- *What technical prerequisites would a transition to a cryptocurrency require?*
- *What major opportunities and limitations would such a transition entail?*
- *What safety concerns are associated with a transition to cryptocurrency?*
- *Could a cryptocurrency supply the functions of a traditional currency?*

The first three questions are posed from a technical point of view with focus on computer security and human-computer interaction. The fourth question will be addressed from a macroeconomic perspective.

The scope of this report has been delimited to exemplify the transition to cryptocurrency using bitcoin, in the purpose of delivering a thorough analysis. The choice to exemplify usimg bitcoin was made since bitcoin is the first, most well-known, and still dominating cryptocurrency. Further on, this report will focus on Sweden, since the Swedes have an outspoken interest for alternative payment methods and technology.

1.4 Evaluation

This report is made with investigatory purposes, hence no hypothesis will be presented. The study will be considered successful if the posed scientific questions have been answered in a satisfactory manner, the definition of which is described below.

- The first question will be considered answered when an analysis of the Bitcoin protocol, as well as a study of the current technological conditions of Sweden, has been presented. Focus will be placed on users and maintenance of the network.
- The second question will be considered answered when an examination of what major possibilities and challenges a transition to a cryptocurrency would imply has been presented.
- The third question will be considered answered when a thorough analysis of the Bitcoin protocol, in relation to the security risks that users of bitcoin are exposed to, has been presented.
- The fourth question will be considered answered when the functions of a traditional currency, and how a cryptocurrency relates to those functions, has been determined.

2 Currencies

The word currency is defined as "a system of money in general use in a particular country" [9]. A currency is mostly known as an accepted form of money that is circulated within an economy, issued by a government. But with time, alternative currencies, explained in section 2.2, have emerged and claimed a share of the currency market.

2.1 The Functions of a Currency

A currency can be summarized by three key functions;

- *Medium of exchange* – Money is used as an intermediary in trades, in order to avoid a system relying on pure barter. To accomplish this function, a currency ought to have characteristics such as recognizably, constant utility, low cost of preservation, transportability and divisibility.
- *Unit of account* – A currency serves as a standard monetary unit of measuring value of goods, services and assets. In order to bring this function to conclusion, a currency needs to be divisible into smaller units without any loss in value. It must also be fungible, meaning that one unit of the currency is equivalent to another unit of the same value, and it must have a specific measure, size or weight in order to be verifiably countable.
- *Store of value* – Money of the currency must remain stable over time. This means that it must be possible to reliably store and retrieve the money over time. [10]

2.2 Types of Currencies

There are several types of currencies, used in different situations and fulfilling different purposes. Those that are relevant for the scope of this report are described below.

2.2.1 Traditional Currency

Traditional currency is physical government issued notes and coins that possess a promise of a future value. A traditional currency fulfils all three functions of a currency and relies on a trust in the central bank providing the money. Traditional currencies are centralized, relying on one institute for money supply and uses banks and other financial institutes for security enforcement and validation. [10]

2.2.2 Digital Currency

Digital currencies are currencies that only are stored and transferred electronically, also called electronic currencies. Digital currencies constitute a broad category that includes both virtual- and cryptocurrencies as well as traditional currency stored in bank accounts. Digital currencies exist purely in electronic form but may be turned into cash by for example making a cash withdrawal at an ATM. Digital money is exchanged and transferred using technologies and has therefore made it possible to bank online, eliminating the dependency on cash or need to visit a bank in person. [11] Today, around 95% of the money is digital world wide [12].

2.2.3 Virtual Currency

A virtual currency is a type of digital currency. Virtual money is not issued by a central bank but relyies on a system of trust. The money can be defined as a digital representation of value that is used in a specific virtual community and issued by the system's developers. One example is the computer game World of Warcraft where the virtual currency, called WoW Gold, may be used for in-game purchases. The virtual currency is made to be a complement to regular money, since it is only used at specific platforms and not in other contexts. Each virtual currency has its own way of functioning, depending on the algorithms, making the foundation of the system, but most of the virtual currencies are centralized. This means that the control of the money supply is centralized to the virtual world's developers. [12]

2.2.4 Cryptocurrency

Cryptocurrencies is another type of digital currency that uses cryptography for security enforcement, making it difficult to counterfeit. What differs cryptocurrencies from virtual currencies is that they are designed to potentially replace traditional currencies. In difference to other currencies, both virtual, digital and traditional, cryptocurrencies are decentralized. This means that there is no central authority or third party controlling the money supply. Cryptocurrencies thus eliminate the need of a central bank, the way most currency markets are structured today. The cryptocurrency that has the largest market share as of April 29th 2017 is bitcoin.

3 The Bitcoin Protocol

The Bitcoin protocol provides both a technical infrastructure, allowing direct online payments, and a cryptocurrency, providing a purely peer-to-peer version of electronic cash. Digital coin transactions have been performed earlier, using digital signatures to sign and verify, providing strong control of ownership. However, there was no solution to the problem of double-spending until Satoshi Nakamoto presented the Bitcoin protocol – a unique combination of technology and advanced mathematics. A protocol with no need of user identification that enables everyone with an internet connection to participate. [1] The underlying technology and use of this protocol will be explored in this section.

3.1 Cryptography

The Bitcoin protocol builds on the cryptographic methods of digital signatures and secure hash algorithms, both explained below. These mechanisms constitute the foundation to the decentralized identity management of Bitcoin.

3.1.1 Digital Signatures

Participation in a bitcoin transactions requires generation of a key pair, consisting of a private key and a public key. The private key is a random number between 1 and 2^{256}, derived in a suitable manner. From this number, a public key is generated with a one-way cryptographic function. Subsequent application of the SHA-256 algorithm, described in section 3.1.2, results in a bitcoin identity called *address*. Figure 1 illustrates the described process and highlights the one-way property. [13]

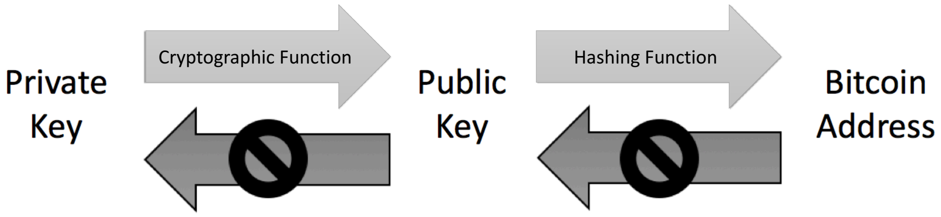

Figure 1. A public key and bitcoin address is created from a generated private key. Neither knowledge of the address nor the public key makes retrieval of the private key feasible due to the one-way property of the algorithms used to derive the address.

In the key pair, the address is used to receive bitcoins while the private key is needed to digitally sign transactions to spend those bitcoins. Consequently, bitcoins are tied to a private key rather than a person. This makes secure key management essential, since revealing or losing a private key would be equivalent to losing control of, or access to, the funds tied to that key. The public key associated with the private key can however be publically distributed, and is used by the network to validate signatures made with the corresponding private key. Usually, key pairs are stored in *wallets*, which are implemented as structured files or simple databases. [13]

The system behind Bitcoin is well-analysed and is generally considered to be secure given today's knowledge of cryptography. However, it is highly dependent on the usage of a good source of randomness, both when the key is generated and when it is used to make signatures. Failure to do so may leak your private key. [13]

3.1.2 SHA-256

The secure hash algorithm used by Bitcoin is called SHA-256, and fulfils the properties that are required by a secure hash function H;

- It takes input of arbitrary length and provides an output of fixed length, in this case 256 bits.
- It is efficiently computable – the hash of an n-bit string is calculated in a running time that is O(n).
- It is one way – given H(x) it is computationally infeasible to find x.
- It is weak collision resistant – given x and y such that x ≠ y, it is computationally infeasible to find H(x) = H(y).
- It is strong collision resistant – given any pair (x, y) such that x ≠ y, it is computationally infeasible to find H(x) = H(y).

In the Bitcoin protocol, the secure hash algorithm is applied twice to the input. This operation is denoted SHA^2 and serves as defence against future cryptanalytic developments. [14]

3.2 Blockchain

The Bitcoin protocol makes use of a data structure called *blockchain* to record transactions. A blockchain, illustrated in Figure 2, is a linked list built with hash pointers instead of regular pointers. Each hash pointer stores the address of the previous block as well as the hash of the previous block's data. Consequently, each block in the blockchain not only contains the location of the previous block, the parent block, but also the hash of the parent block's value. This goes back to the very first block in the chain, the genesis block. The genesis block is statically encoded within the bitcoin client software and functions as a secure root to build a trusted blockchain from. [14]

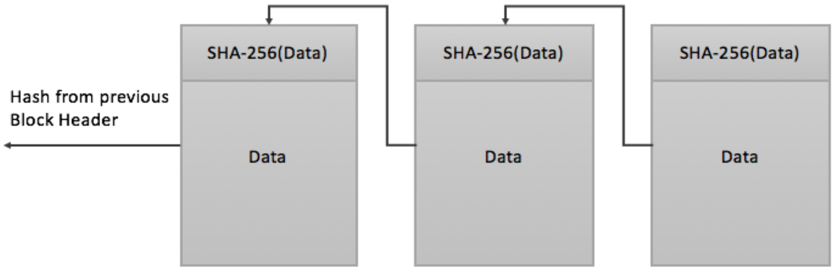

Figure 2. A blockchain constitutes of blocks of data. Each block contains the hash of the previous block's data, going back to the genesis block, and thus allows for consistency validation.

In the Bitcoin protocol, the blockchain serves as a ledger, a record of every existing bitcoin and bitcoin transaction ever made. As new transactions take place, new blocks are added to the end of the chain. Because of the structure of the blockchain, a transaction is considered tamper-evident when there are at least six blocks between the current block and the block the transaction in question is included in. This because an attacker wishing to alter a transaction would have to traverse through the blockchain and modify all the succeeding blocks' hash pointers, in order to create consistency in the ledger. The longer the blockchain becomes the more processing power is required for such an operation. Alteration of a transaction more than six blocks deep consumes more processing power than one attacker is assumed to be able to control. [14]

3.2.1 Block Structure

Each block in the blockchain consists of a header followed by a list of transactions. The block header contains three pieces of metadata; a reference to the parent block hash which connects the block to the previous block in the chain, the difficulty, timestamp and nonce - information pieces related to the *Proof-of-Work* algorithm discussed in section 3.5.1, and last the merkle tree root. [13]

A Merkle tree, exhibited in Figure 3, is a binary tree constructed with hash pointers instead of regular pointers. Each transaction in the block is represented by a leaf in the tree, and consecutive leaf nodes are then summarized into a parent node, using the SHA-256 algorithm. This propagates to the top of the tree, the merkle root, which is as a compressed summary of all transactions in the block. The merkle root is a cryptographic proof of what transactions are included in the block, and in which order those transactions occurred. On average, more than 500 transactions are included in a block, each consuming at least 250 bytes. This can be put in relation to the merkle root, which is always 32 bytes, independently of the number of transactions included in the block. [13]

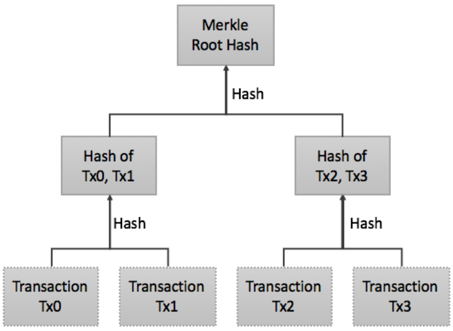

Figure 3. A Merkle tree constitutes of transactions, efficiently summarized in the merkle root.

There are two ways to identify a block – by referencing the block hash or the *block height*. The block hash is the result of applying the SHA-256 algorithm twice to the block header. The block hash is unique and as such identifies a block unambiguously. Each block is also numbered after its position in the blockchain, starting from the genesis block at height 0. However, the block height is not guaranteed to be a unique identifier because of a phenomenon called blockchain forks, explained in section 3.5.2. [13]

3.3 The Network

Instead of relying on a central authority for transaction verification, the Bitcoin protocol relies on a resilient, decentralized and open peer-to-peer network. The network refers to the *nodes* running the system peer-to-peer, forming a loosely connected mesh where all the nodes have their own copy of the ledger. The nodes need not to be identified to enter the network and may leave and re-join the network at any time. [1] The responsibility of the nodes is to validate and propagate blocks and transactions as well as to maintain connections to peers. All nodes are equal but may play different roles in the network by possessing different combinations of the four node functionalities; wallet, miner, full blockchain database and network routing. A so called full node possesses all the functionalities and thus maintains an up-to-date copy of the complete blockchain, hence the full nodes can authorize and autonomously verify transactions, without references from others. Other nodes, called SPV or lightweight nodes, may possess all the functionalities but "full blockchain database". Instead they maintain a subset of the blockchain and verifies transactions by a method called Simplified Payment Verification (SPV). With this method, the node downloads only the headers of the blocks. To verify a transaction, the SPV-node hence needs to request the block's complete list of transactions from a full node. [13]

The nodes are connected via TCP and in order for a new node to get connected and gain the possibility to participate, it must discover at least one existing Bitcoin node, such as one of the long-running stable nodes listed as seed nodes. When connected, the new node will send a message containing its IP address to the adjacent nodes, who in turn forwards the message, to ensure the node gets widely connected. [13]

3.4 Transaction Verification

One of the most important responsibilities of a node is to verify transactions. When a new transaction is broadcasted on the bitcoin network, the nodes validate it against a long list of criteria. If one of the criteria is not fulfilled, the transaction is rejected. When a transaction is considered valid, the node propagates it to its peers, illustrated in Figure 4. This process is individually performed by the nodes until the transaction, if valid, has reached every node in the network. As long as the network consists of a majority of honest nodes, not cooperating, the network is able to prevent invalid transactions from ending up on the ledger, which Figure 5 highlights. The security is enforced by honest nodes, not propagating invalid transactions to its neighbour nodes, and by mining nodes, not including invalid transaction in their candidate blocks. [14]

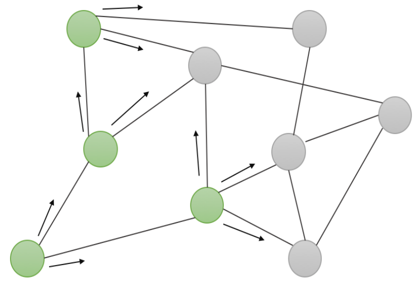

Figure 4. If a transaction is considered valid, an honest node will approve it and propagate the transaction to its peers. This is illustrated with a green dot.

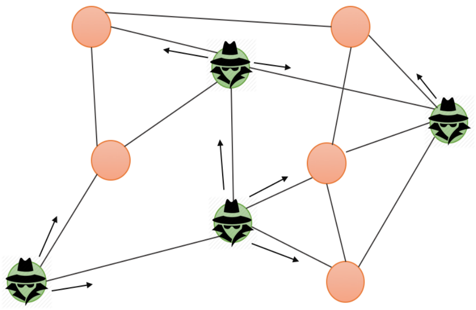

Figure 5. If a dishonest node, illustrated with a man in hat, propagates an invalid transaction, an honest node will reject the transaction and not propagate it to its peers. This is illustrated with a red dot with no outgoing arrows. Dishonest nodes in cooperation will propagate the transaction, but as long as there is a majority of honest nodes on the network, the invalid transaction will be rejected by the network.

3.5 Bitcoin Mining

Bitcoin mining refers to the process of adding new bitcoins to the money supply, which occurs when new blocks are created. Thus, the mining process serves as a decentralized clearinghouse, validating and clearing transactions. Mining is one of the four functionalities that a node may possess and technically, anyone can be a *miner*, but since the activity is most efficiently done by highly specialized processors, it is associated with high costs. Consequently, the power of the mining ecosystem has become centralized to a smaller group of nodes. [14]

When a mining node receives a valid transaction, the node includes it in its own transaction pool, a candidate block filled with verified transactions. The mining nodes of the network will all have slightly different ideas of what the next block will look like, depending on what transactions has been propagated to them at that time. Mining nodes will compete against each other in solving a so-called *hash puzzle*, described in section 3.5.1, to have their candidate block added to the blockchain. When a solution is found, the node broadcasts its block to the network. The proposed block is accepted by the other nodes if all included transactions are valid, if the coins are unspent and the signatures are accurate. The nodes express their acceptance of the block by including its hash in the next block they create as well as adding the block to their own version of the ledger. [14]

3.5.1 Proof-of-Work

To construct a block and propose it to the network the miner must solve a hash puzzle. The puzzle is to find a random number, called nonce, that solves the following inequality:

SHA-256^2 (nonce || previous_hash || transaction || transaction || … || transaction) < target

Miners generate and try nonces one by one until a successful combination is encountered. The double hash of the concatenation of the nonce, the previous hash and all the transactions in the node's candidate block is considered successful if it falls in a pre-defined target space. [15]

The solution to the hash puzzle is called Proof-of-Work and is included in the newly created block. The solution serves as proof that the miner spent substantial computing power mining the block. The difficulty of the hash puzzle, that is the size of the target, is automatically adjusted by the network to ensure that the mining ecosystem produces a new block approximately every 10 minutes. [15]

Since miners compete in solving the hash puzzle simultaneously, independently from each other, it occasionally happens that multiple nodes solve the current problem at roughly the same time, creating multiple blocks at the same height. This phenomenon is called blockchain forks. [13]

3.5.2 Blockchain Forks

Figure 6 illustrates the occurrence of two mining nodes having solved the hash puzzle at the same time and broadcasted their different blocks to the network, identified with the same block height.

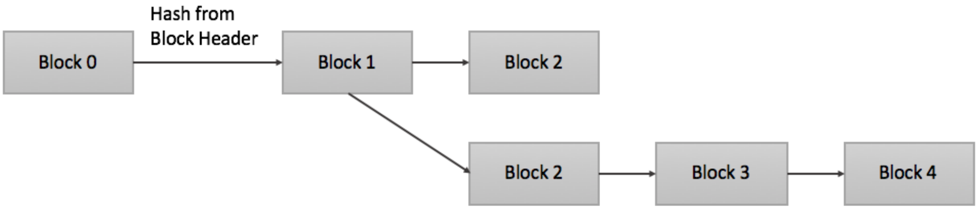

Figure 6. When two mining nodes solves the hash puzzle at roughly the same time, two blocks with the same height are created with the result of two branches.

The nodes of the network always work on extending the longest chain of the blockchain but when there are multiple valid blocks to choose among at the end of the blockchain, the nodes usually keep working on the first one they receive. Eventually, there will only be one mining node solving the next hash puzzle, producing a single block to add to the blockchain, making one branch longer and stronger than the other, eliminating the fork situation. [15]

3.5.3 Mining Rewards

As reward for mining, nodes receive a block reward and transaction fees. These two mechanisms are implemented to serve as incentives for nodes to behave honestly.

The block reward refers to a special transaction that the node who mines a block gets to include in that block. The transaction is a coin-creating transaction to a recipient address of the node's choice. The block reward, currently at 12.5 bitcoins, serves as payment to the node for expending its processing power. The block reward originated at 50 bitcoins, but is programmed to half with every 210,000 blocks created, which occurs approximately every four years. Mining is the sole process of creating bitcoins and subsequently, there is a finite number of bitcoins that can be issued – nearly 21 million. This amount is asymptotically approached, and is estimated to be reached in year 2140. [13]

In order for the node to collect its reward, the coin-creating transaction must be considered confirmed, a state reached first when the transaction is validated and accepted by the other nodes in the network. This incentivizes nodes to act in an honest way to maximize the probability of their mined block being accepted by the network, so that the mining node can be compensated for expending its processing power. Since a block containing invalid transactions won't be accepted by the network, this incentives the nodes to behave honestly. [14]

By making the total value of the transaction inputs larger than the total value of the transaction outputs, the payer generates a transaction fee that the node who mines the block that first adds the transaction to the blockchain may collect. The transaction fee is not mandatory but transactions with transaction fees are prioritized by the mining nodes, who in self-interest strives to maximize profits. As the block reward continues to decrease, transaction fees are expected to almost become obligatory to get transactions validated in reasonable time. [14]

3.6 Consensus

The network needs to establish trust and achieve global consensus without relying on a central authority, therefore the Bitcoin protocol relies on a decentralized mechanism for emergent consensus. It is emergent since consensus is not achieved at a fixed moment, but through the interaction between the nodes following the below four processes, independently performed across the network:

Every node independently verifies each transaction based on a comprehensive list of criteria:
When a node receives a transaction request, it verifies it against the list of criteria and if some criteria is not fulfilled, the transaction is rejected. An honest node only propagates valid transactions.

Mining nodes independently aggregate transactions into new blocks that are made valid for the blockchain by computing a solution to the Proof-of-Work algorithm:
The mining node collects verified transactions in a candidate block and will work on finding a solution to the Proof-of-Work algorithm for this block. When a solution is found, the new block is broadcasted to the network.

Every node independently verifies and approves new blocks. If valid, the new blocks are put on the node's blockchain ledger and if invalid, the blocks are rejected:
When a solution to the Proof-of-Work algorithm has been found and the new block has been broadcasted to the network, every node independently performs a series of tests to validate the proposed block. If the new block is considered valid, each node will put it on its copy of the blockchain ledger and propagate it to its neighbour nodes. If the block is not considered valid, the node will reject it and the proposed block can never become part of the node's ledger.

Every node independently selects the longest chain:
When a block has been added to the blockchain, the mining nodes will keep working on extending that chain. The mining node will start working on a new block and drops all the transactions that was included in the block last added on the chain from its transaction pool. By always selecting the chain of greatest length, all nodes will achieve network-wide consensus.

These four processes are the foundation of creating a network-wide consensus and allows any node to possess its own copy of the trusted global ledger. [14]

4 Method

This report is based on a literature study and a semi-structured interview with Björn Segendorf at the Swedish Riksbank. The literature study included a comprehensive collection of different media such as scientific articles, nonfiction books, statements, debate articles and exploring reports. The comprehensive media base gave a detailed understanding of an area not deeply charted in academic literature. The studied media covered cryptocurrencies in general as well as the underlying technology, security and the potential opportunities and limitations of the Bitcoin protocol. Further on, the studied media covered the usability of cryptocurrencies and the technical prerequisites for managing a cryptocurrency. The definition of a currency, as well as the macroeconomic perspective on cryptocurrencies, were investigated. The interview with Björn Segendorf aimed to determine the Riksbank's interest and opinion in these matters, wherefore the asked questions were open in order to get broad answers. Topics covered in the interview were; the security of the Bitcoin protocol, the effect an implementation of a cryptocurrency would have on the user, the modern use of different means of payment and the future of Bitcoin, cryptocurrencies in general and the Riksbank.

To answer the first scientific question, the technical prerequisites of implementing and maintaining Bitcoin was studied. In order to determine the technical development and the current technical state in Sweden, statistics from available market research was collected. To answer the second and third scientific questions, the Bitcoin protocol was examined in detail and analysed from a usability perspective, both on an individual and on a societal level. To answer the fourth scientific question, literature focusing on both economics and bitcoin was studied. The interview with Björn Segendorf gave a comprehensive picture of the Riksbank's opinions in all the studied areas.

The implementation, use and expansion of cryptocurrencies have, from the beginning, met various reactions. As of today, there are still different opinions about most subjects regarding cryptocurrencies. Hence, to obtain the entire picture, a deliberate choice was made to include material from both the pro and con side of all areas.

5 Result

5.1 How Cryptocurrencies Meet the Currency Prerequisites

A currency needs to fulfil the three functions, described in section 2.1, namely Medium of Exchange, Unit of Account and Store of Value. Below follows an analysis of the level of fulfilment of these prerequisites for cryptocurrencies in general and bitcoin in particular.

5.1.1 Cryptocurrencies in General

When talking about cryptocurrencies as a concept, one needs to take into consideration that there exist over 800 different cryptocurrencies. Each has different algorithmic structures, target groups and underlying technologies. Therefore, the analysis below will be made for cryptocurrencies in general.

Medium of Exchange:

In theory, a cryptocurrency could fulfil all the criteria for functioning as a medium of exchange, as long as the currency gets widely known, has a constant utility, has a low cost of preservation, good transportability and is divisible. This depends on the cryptocurrency, but in general cryptocurrencies are divisible and easy to transfer, since they are completely digital. A cryptocurrency is expending memory rather than physical space, as cryptocurrencies are stored "in the cloud", on the internet or on different hardware rather than in a bank vault. Today, the cryptocurrency that is most widely known is bitcoin [13].

Unit of Account:

To fulfil the criteria of being a unit of account, the cryptocurrency must be an accepted measurement of value. Today the use of cryptocurrencies for measuring value is very limited. Goods, services, loans and assets are rarely expressed in terms of cryptocurrencies, even though it might be posed as a payment method.

Store of Value:

Whether cryptocurrencies, in general, could be said to be stable over time is hard to say, as there are over 800 cryptocurrencies with exchange rates depending on predictions, rumours and exposure affecting the supply and demand. Today, cryptocurrencies are however generally considered to be very volatile, making them insufficient as store of value.

5.1.2 Bitcoin Exemplified

Bitcoin is the most common and widely spread cryptocurrency on the market. Whether bitcoin fulfils the three functions of a currency is analysed below.

Medium of Exchange:

In theory, bitcoin fulfils the criteria for functioning as a medium of exchange. The currency is quite widely known since according to a study made in 2015 at the Royal Institute of Technology, 91% of the participants had heard of bitcoin, though only 13% had used it for payments [16]. Bitcoin has low costs for preservation, since the coins are stored purely on the blockchain which is stored on the nodes' hard drives. Transferring coins is easy since the information of the coins is accessible to everyone. To make a transfer, the sender simply passes the control of the coins to the receiver. The bitcoins are also divisible into so called *satoshis* where one satoshi is one hundred millionth of a single bitcoin [17]. Hence bitcoin fulfils the functions of being a medium of exchange.

In practice, bitcoin is used as a medium of exchange, but to a limited extent. The usage is spread all over the world but is rather limited. The role as a medium of exchange relies on the fact that the medium is widely accepted by the society, and though the usage is limited, the acceptance of bitcoin is growing. In mid-2014 there were about 65,000 merchants accepting bitcoin as a medium of exchange, increasing to 100,000 merchants in mid-2015, showing a growth in acceptance [18].

Unit of Account:
In Sweden, it is possible to pay with bitcoins at 39 retailers [19]. Hence bitcoin is a very rarely used unit of account in Sweden as of today, though it happens. When using bitcoin as a unit of account, it is mostly used for measuring value of goods or services rather than assets or loans. Even where payment in bitcoins is accepted, prices are mostly written in the local traditional currency rather than the cryptocurrency.

Today bitcoin is considered more of an actual asset than a unit of account for measuring the value of an asset [36]. But it is divisible, as stated above, and the use of bitcoin is constantly growing with increasing possibility to use bitcoin for payments.

Store of Value:
Bitcoin is very volatile. As illustrated by Figure 7, the exchange rate of bitcoin has shifted a lot during the last year. The exchange rate of bitcoin is affected by speculations, regulations and rumours, making the rate swing hardly. While these factors influence other exchange rates as well, the fluctuations of traditional currencies are of less amplitude, a phenomenon pictured in Figure 8.

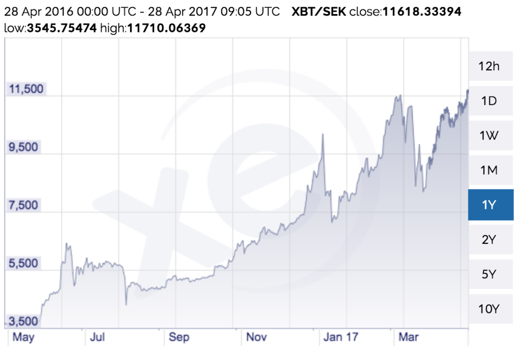

Figure 7 [20]. The bitcoin/SEK exchange rate has shifted between 3,500 SEK and 11,600 SEK the last year.

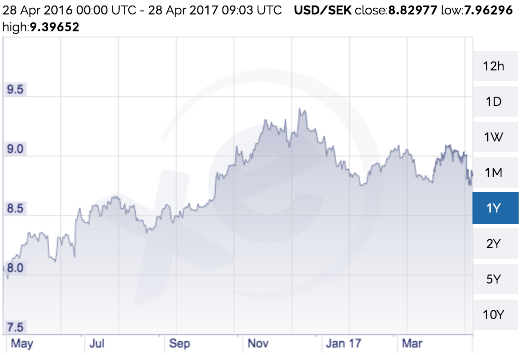

Figure 8 [21]. The USD/SEK exchange rate has shifted between 7.96 SEK and 8.3 SEK the last year.

The fact that the bitcoin exchange rate is so volatile might be one reason of why prices are rarely measured in bitcoin. The volatile exchange rate makes bitcoin inappropriate as a store of value, since a bitcoin is unlikely to have the same value tomorrow as it did today. Though bitcoin is volatile, it is handling fluctuations more calmly than it did a couple of years ago, indicating a trend of maturity. [22] This argument will be explained in depth in section 5.6.3.

5.2 Technical Prerequisites for Managing a Cryptocurrency

To be able to use Bitcoin, there are several technical prerequisites that need to be fulfilled. These differ depending on the participant's role in the network, but a common feature is the need of an internet connection.

5.2.1 The User and the Merchant

From a user's perspective, Bitcoin is no more than another computer program or a mobile application maintaining a wallet for storing keys and making bitcoin payments. There are several distributors offering various wallet services, all using software following the same rules in order to reach consensus throughout the network. The wallet can be maintained on a smartphone, desktop, hardware or virtual on the web. Common to most wallet solutions, is that they require some sort of technological device. According to statistics collected in 2016 [23], 93% of the Swedish households had access to internet. 92% of the Swedes had access to a computer and 81% of the Swedes owned a smartphone. These numbers show that Sweden is at the technological forefront with a comprehensive spread in the use of internet and electronic devices.

In order to accept payments with bitcoin, a merchant needs to have a set of technical devices. Special hardware terminals, touch screen applications and QR readers support bitcoin and make it possible for merchants to accept bitcoin as a payment method. [24]

5.2.2 The Network Participants

The network members maintaining the Bitcoin network, such as verifying transactions and mining, require more advanced technology than a user or a merchant does.

At first, anyone could run a mining node, using only the CPU power of their personal computer. As the difficulty of the Proof-of-Work algorithm has increased over the years, the CPU power required for solving the hash puzzle has increased, making it necessary to have specialized hardware in order to maintain a mining node that does not cost more in electricity than earned in bitcoin. [25]

Running a full node currently requires 125GB of free disk space, 2GB of RAM memory and a broadband connection with uploading speeds of at least 400Kbit per second [26]. In 2016, most computers in Sweden had a RAM memory of more than 2GB and the average broadband connection speed for uploading was 35Mbit per second [23].

5.3 Opportunities Created by the Bitcoin Protocol

The technical infrastructure of Bitcoin creates opportunities that cannot be observed in the modern payment systems of today. Following is a brief description of the major opportunities of this kind.

5.3.1 Open Participation

Cryptocurrencies in general, Bitcoin included, allows anyone with an internet connection to participate. This open participation is enabled since Bitcoin is built entirely on verification, eliminating the need of trust. Modern financial institutes and other intermediaries do not possess this possibility due to regulations and industry structure. To open a bank account in Sweden, there are certain requirements, such as being able to present a valid ID document. Cryptocurrencies give groups, that for various reasons are excluded from the traditional financial infrastructure, access to a technical payment system.

5.3.2 Time and Cost Efficient Transaction Processing

An additional limitation of traditional payment methods is the complexity of cross-system interaction. Making cross-border transactions and bank-to-bank transfers consumes 1 to 5 banking days and eventual transaction fees. Bitcoin offers a technical infrastructure to transfer money anywhere in the world at any time. Since both parties are connected to the same network, borders are eliminated. No matter where on the globe one is located, transactions can be validated and confirmed within the hour, as long as payer and payee have access to a Bitcoin software. Consequently, the technical infrastructure presented by cryptocurrencies compares to the traditional payment systems as notably more time and cost efficient in this area. [3]

5.3.3 Preservation of Payer Integrity

Further on, Bitcoin transactions are always initiated by the payer and does not disclose any personal or sensitive information. This feature provides the payment system technology behind Bitcoin with two key strengths that traditional payment systems lack.

First, the payer's protection against identity theft is strengthened since no sensitive information must be revealed to the payment recipient or to any other entity. The payer only needs the payee's bitcoin address to initiate a payment, and similarly the payee, besides access to the transferred bitcoins, only receives information of the payer's bitcoin address. The one-way property of the algorithm utilized to derive addresses, described in section 3.1.1, assures that knowledge of a bitcoin address cannot be used to defraud the owner. [17]

Credit card transactions on the contrary, are initiated by the payment recipient and thus require the payer to disclose their credit card information to the recipient. Consequently merchants, and eventual third parties that are involved in the transaction, are responsible for the payer's financial security. This arrangement can be costly and resource demanding for merchants, and enervating for customers that must risk compromising their personal information every time they want to make a payment.

Second, traditional payment methods create a possibility for merchants to draw money from the payer's account without the payer's consent. In Bitcoin, this is not an issue since payments are always initiated by the payer. Bitcoin offers an additional upside for merchants as well, who do not have to worry about cancelled payments or chargebacks due to the finality of bitcoin transactions. [17]

5.4 Limitations of the Bitcoin Protocol

The literature study has also pointed out some limitations of the Bitcoin protocol. These may pose an obstacle for a more extensive use of the protocol. Following is a brief description of the major limitations of this kind.

5.4.1 Scalability Limitations

The Bitcoin protocol currently restricts the block size to 1MB. The purpose of this restriction is to fasten block propagation and to reduce anomalies. As a result, Bitcoin can process an average of 7 transactions per second. According to the Riksbank, approximately 7 to 8 million card payments are conducted daily in Sweden [8]. This corresponds to an average of 87 transactions per second, assuming those transactions are evenly distributed during the day. In reality, a majority of these transactions can be expected to occur between 7am and 10pm - the opening hours of most Swedish grocery stores and when a majority of the Swedish population is conducting business. Concluding, the total transaction demand is expected to be closer to an average of 139 transactions per second, and is likely to peak during rush hours. To satisfy Sweden's transaction demand, Bitcoin would thus need to scale notably.

There are ongoing debates on how the network should scale. A proposal to increase network throughput called Segregated Witness was introduced in December 2015 by developer Pieter Wuille. Wuille's idea is to store transactions more space efficiently to fit 1.8 times more transactions into one block. In order for the network to scale to throughput volumes that would meet a transaction demand the size of Sweden's, most developers however agree that the allowed block size will have to increase. [27]

The literature study charted different stakeholders in the block size debate. The pro side argues that transaction fees will drop as a result of larger block sizes and that it will leave space for altcoin extensions. On the other hand, some express worries that the propagation speed will slow and that the risk of double-spending attacks consequently would increase. Any update of the protocol may be implemented and adopted if the presented solution reaches network consensus, a state reached if a large majority of the network's computing capacity considers the update beneficial. [28]

5.4.2 Confirmation Times

The way the Bitcoin protocol is constructed today, a transaction is considered final roughly an hour after its initialization. This phenomenon, described in section 3.2, could be a limitation in some payment situations. Over the counter payments in its modern form is an example of a situation that is not compatible with slower transaction speeds, as goods and services are expected to be exchanged for monetary value in real time. Modern card payments solve this issue by reserving the amount on the payer's account and avouching that amount for the recipient [29]. In Bitcoin's decentralized network, there is no central party that can provide such a warranty. A market for payment service providers that guarantees bitcoin payments between payer and payee, and thus disengages the parties from the counterparty risk that the confirmation retardation entails, emerges. However, usage of such central parties contradicts the core idea behind Bitcoin as a decentralized payment system.

5.4.3 Energy Consumption

The high electricity consumption of the mining process has also been appointed as a possible limitation of the further growth of Bitcoin. Each miner expends substantial computing power whilst competing to find a solution to the Proof-of-Work algorithm, described in section 3.5.1. Studies conducted in 2014 shows that the power used for bitcoin mining is comparable to the electricity consumption of Ireland with its 4.5M inhabitants [30]. Consequently, scaling of the bitcoin network might not be defendable due to global resource constraints.

Naturally, maintenance of the traditional payment systems also consume energy on services such as issuing and distributing cash, running bank offices and providing credit and debit card services. The energy consumption of these services is however not as transparent as the one of the Bitcoin network, and is thus difficult to quantify.

5.5 The Security of the Bitcoin Protocol

The security of the Bitcoin protocol is generally considered high but is dependent on some key factors, described below.

5.5.1 Decentralization of the Mining Ecosystem

In the Bitcoin network, computing power is used to vote with. As a result, it is significant that a majority of the mining power is controlled by honest nodes. In a decentralized system with no responsible issuer, the only way to guarantee this is to make sure the network's total computing power is large enough to make it infeasible for an attacker to gain control over more than 50%.

Today, the bitcoin mining ecosystem is relatively centralized. This is due to three factors. First, the threshold to enter the mining field is high as the required hardware is costly. Second, the profit is variable and hard to estimate while costs are fixed, which makes mining associated with high risk. The miner's profits consist of the mining rewards and transaction fees, both only obtained when the miner succeeds in adding a block to the blockchain. To have a chance at making profit, the miner needs computing power, which consumes electricity. Further on, the hardware needs to meet the ever-increasing standards of the network. A third complication is that the profits are denominated in bitcoins, while the costs usually are denominated in a traditional currency. This exposes the miner to fluctuations in bitcoin's exchange rate. [14]

As a consequence of the mining industry's complexity, the number of miners is relatively low. A growth in the number of miners cannot be expected unless mining becomes more profitable. This scenario may become reality if hardware and electricity costs decrease, but as the number of miners increased, the hash puzzle's difficulty would be adjusted, and the profits would drop. This would make it less incentive to enter the mining ecosystem, wherefore the temporary network expansion would cease. Long-term, the mining industry is thus expected to be in economic equilibrium with a stable number of miners. [14]

If this number drops too low, making a 51%-attack possible, the system is at risk. The way the consensus protocol is designed, the damage a potential 51%-attacker could do is limited. A probable outcome is a blockchain fork, described in section 3.5.2, that is a split of the blockchain into one valid fork and then the attacker's invalid fork. The attacker could do anything with the invalid branch, for example include invalid transactions and create new bitcoins, but would in reality not be able to benefit from this since no honest node would keep building on this branch. Instead, the honest nodes would extend the valid branch. As a result, the attacker would not be able to spend the falsified bitcoins. [14]

The news itself, that 51% of the mining power is controlled by one party - honest or not, constitutes a larger threat to the system. The world's trust in the Bitcoin protocol would be compromised, since such news would implicate that Bitcoin has become just as centralized as the systems it was supposed to improve on. This would likely be the end of Bitcoin, since it would make the exchange rate drop and put bitcoin assets at a zero intrinsic value. [14]

5.5.2 Existence of Full Nodes

Another security threat, pointed out in the literature study, is the size of the blockchain. As stated in section 3.3, a full node fully validates transactions and blocks by possessing a full and complete copy of the blockchain. The full nodes also serve as intermediaries between other nodes in the network by broadcasting valid transactions to all their peers. As SPV nodes, described in section 3.3, does not possess a copy of the full blockchain, they rely on full nodes for complete transaction verification and broadcasting. Therefore, if there are not enough full nodes able to perform their function, peers will not be able to connect to each other. Hence, as Bitcoin continues to grow the number of full nodes will need to increase in order to maintain the decentralized network that Bitcoin relies on. However, running a full node comes with costs which creates a dilemma.

The blockchain expands whenever a new block is accepted by the network and added to the blockchain. Since a new block is added roughly every ten minutes and a block is less than 1MB, this means that the blockchain could grow with a maximum of 51GB per year, if every block is of maximum size. Hence, storing a copy of the full blockchain on your device takes up a lot of free space. Today the blockchain is 109GB and it is increasing linearly [31]. Due to this, the threshold for becoming a full node enlarges and the incentives for the existing full nodes maintaining the blockchain are reduced.

Running a full node comes with certain minimum requirements in terms of free memory, hardware and broadband internet connection. As stated in section 5.2.2, running a full node currently requires 125GB of free disk space, 2GB of memory and a broadband internet connection that have uploading speeds of at least 400Kbit per second. Due to the blockchain growth, these requirements will augment and expenses increase, causing a decline in the number of full nodes [32]. A decreasing number of full nodes forces the network into becoming more centralized which, as stated in section 5.5.1, is a threat to the security of using Bitcoin.

However, there are several proposed solutions to this problem. One of them, mentioned by Satoshi himself in his white paper, is called pruning. To reclaim disk space, Satoshi means that once a coin is completely spent, the earlier transactions of that coin can be discarded. A coin is considered completely spent when the latest transaction of the coin is buried under enough blocks. As the transactions are hashed in a merkle tree with only the root included in the block header, explained in section 3.2.1, discarding transactions can be done without breaking the blocks' hash and the security would therefore be maintained. As a block header is about 80 bytes, with no transactions included, this would result in the blockchain growing 4.2 MB per year. [1] This technique is used by the SPV nodes and enables more nodes to become part of the network, due less disk space consumption. While this makes the network more decentralized, there is still a need of full nodes possessing a copy of the full blockchain. As the number of full nodes would decrease with pruning, the network would need to place more trust in each.

5.5.3 User Integrity

All transactions, containing information about the sending and receiving bitcoin addresses and the number of bitcoins being transferred, are registered on the blockchain, making Bitcoin a transparent payment system. Since the blockchain is publically available on the Internet, anyone can retrieve and analyse the transaction history and trace every single bitcoin – from creation to current holder. Consequently, this data creates the possibility to determine the balance and transaction history of every single bitcoin address registered on the blockchain.

Since a responsible issuer is absent, it is every user's personal responsibility to adopt proper integrity preserving routines. To preserve integrity, users must make it infeasible for others to tie them to their wallet. In theory, this means not to disclose one's bitcoin address. However, a user will be tied to his bitcoin address quite frequently – almost all bitcoin exchanges and merchants require at least parts of your personal information to perform the purchased service. The Bitcoin community recommends users to utilize a new bitcoin address for every received payment, and further on to use different wallets for different purposes. If users succeed at hiding the connection between their real-world identity and their bitcoin wallet, their transactions will remain anonymous. Failure to do so will however result in their transaction history becoming available to any interested party. [3]

Today, it is unlikely that even a minority of the Swedish population would be able to use Bitcoin in an integrity preserving way. This since the safety mechanisms developed by the Bitcoin community are quite complex. According to Segendorf [8], Swedes are custom to trusting the payment system without having to understand the underlying technology. There are current research and projects dedicated to developing more user-friendly integrity functionality, a key point to solve before the cryptocurrency can be expected to interest the masses.

The possibility to make anonymous transactions attract some groups, such as criminals. This creates a societal problem since authorities cannot monitor or trace neither transactions, nor goods and services, to the same extent as traditional payment systems allow. On a societal level, this is another important issue to tackle before implementing a cryptocurrency.

5.5.4 User Safety

The absence of an issuer also places the user's financial safety in the hands of the user. This feature is highly appreciated by most Bitcoin users, but could constitute an obstacle for the everyday person since the Bitcoin protocol is only safe given it is used correctly. Users that fail to protect and keep their private keys will forever lose access to the funds tied to those keys. It is impossible to know how many bitcoins have been lost over the years, but there are numerous examples of people losing their money to fraud or by accident [4].

In this context, funds placed within the traditional financial infrastructure are more protected as they are covered by laws and regulations. Since there exists no responsible issuer of bitcoin, the cryptocurrency is not covered by the Swedish law, simply because there is nowhere to turn concerns or complaints to. [29]

5.6 Bitcoin from a Macroeconomic Perspective

Bitcoin not having a central issuer also impacts the macroeconomics. Macroeconomic theory can be divided into several schools of thought [33], such as the Classic and Neoclassic school, the Keynesian school, the Monetarist school and the Austrian school. The schools have different views on how the market and its participants operate and how an optimal economy is achieved.

5.6.1 The Austrian School of Economy

During the conducted literature study, the Austrian school of economy has often been mentioned in the same contexts as cryptocurrencies, and bitcoin especially. The Austrian school of economy is one of the older schools of economics and is based on the idea that all social phenomena is the result of actions and motivations of individuals. In difference from the other schools of thought, the Austrian school claims that models for human behaviour based on mathematics and collected data will be inaccurate, as the human behaviour is too idiosyncratic. [33] The Austrian school also claims that minimal government intervention is optimal for the economy and therefore criticizes the current fiat money system. In the book “The Free Market and Its Enemies” from 1951, the Austrian school economist Ludwig von Mises claims that we need to return to the gold standard. Mises states that “a fiat money system cannot go on forever and must some day come to an end” and that ”the question is how to return to the gold standard”. [34]

The theory and foundation of Bitcoin share some similarities with the Austrian school of economics. Like the Austrian school, Bitcoin also criticizes the fiat money system and the need of a central authority for money supply. Both parties also criticize the fractional-reserve banking system where banks extend their credit supply above their reserves. The Austrian school of economy claims that we need to return to the gold standard, and bitcoin has several times been referred to as the digital gold of today, possessing many of the advantages of real gold such as the benefits that comes from the scarcity. [35]

Although Bitcoin seems to follow the scheme found in the Austrian school of economics, criticism towards Bitcoin has been stated among some of the Austrian economists during the years. The critique focuses on bitcoin’s fluctuating value, which makes it inappropriate as gold substitute. However, Austrian economist Trace Mayer states that economists and capitalists nowadays seek safety and liquidity that the traditional fiat money system cannot provide. Mayer claims that bitcoin has no counterparty risk, is equity based, is more portable than gold and has never become worthless during its existence. Hence, Bitcoin might be a good alternative to gold. [36]

5.6.2 Maintaining a Stable Economy

Macroeconomic policy is used to stabilize the economy and can be divided into two sub policies; fiscal policy and monetary policy. Fiscal policy is most often managed by the government while monetary policy is managed by the central bank, or another equal party. The policies are used to influence the macroeconomic conditions. Whether economic manipulation is considered beneficial or not, depends on what school of economy one belongs to. The Keynesians believe that controlling the money supply is a key tool in managing a sustainable economy whilst the Austrian school of economy claims that economic manipulating is harmful for the economy. [37]

The government manages fiscal policy in attempt to keep the level of unemployment low, to control inflation, influence interest rates and to stabilize business cycles. By changing the tax rates and increasing the government's spending, they hope to increase the customer spending to fuel economic growth. A transition to bitcoin would not have a large impact on the government's possibility to conduct fiscal policy, but rather affect the monetary policy. [38]

In Sweden, the monetary policy is managed by the Riksbank with the aim to maintain a low and stable inflation rate, discussed in depth in section 5.6.3. This is managed by changing the interest rate and controlling the size and growth of the country's monetary supply. The value of government issued money relies on the full faith and trust of the government and central banks who issue them as traditional currencies are not backed up by any actual reserve or tangible asset. Money may therefore be created in any amount, depending on monetary policies in attempt to stimulate the economy. The traditional system also enables the government to track currency movement and therefore collect taxes on profits as well as tracing criminal activities. As the trust for banks and traditional currencies decrease, market participants seek alternatives such as cryptocurrencies. [38]

Since Bitcoin does not have an issuer, bitcoin transactions are neither taxable nor traceable in the same way as traditional currency transactions. The coin supply is strictly limited to the mathematical rules stated within the Bitcoin protocol itself, following a predetermined scheme. The fact that the coin supply of bitcoin cannot be controlled makes it impossible to issue extra money to please political decisions. Therefore, a transition to cryptocurrencies could be seen as a threat to central banks, not because they would be replaced, but because cryptocurrencies may eliminate the need of a central bank as it functions today. [39]

As of today, Björn Segendorf at the Swedish Riksbank does not see the emerge of cryptocurrencies as a threat to their business. Segendorf thinks that most of the time, new technology creates a possibility to meet the needs in an economy. A cryptocurrency like bitcoin could contribute to a more stable payment system since not all payments go through the traditional payment system, which is considered positive from a perspective of continuation [29]. But since it is a new technology, Segendorf thinks that it might change the financial industry, affecting the monetary policy and financial stability, hence creating unexpected risks. The Riksbank is considering creating a digital currency of their own called e-krona, which could be a complement to the traditional currency SEK that Sweden has today. [8]

5.6.3 Controlling the Inflation

Bitcoin's fixed supply is a key discrepancy from traditional fiat currencies, the monetary base of which is adjusted by central banks to match the growth of the economy. The purpose of this is to maintain a mild inflation, the goal established by the Swedish Riksbank is 2% [40], since most central banks assert this a necessity to trigger spending and investments – key ingredients in a growing economy. Failure to do so would, according to some theorists, cause an economic downturn.

The Austrian school of economy suggests that only the purchasing power of money is relevant, and that an economy can be run on a monetary base of any size. A fixed money supply, like that of bitcoin, should thus not be considered a limitation. Since the monetary base cannot be expanded, economic growth will result in a price drop of goods and services, allowing purchases of larger quantities for equivalent amounts. Keynesian economists claim that deflation is harmful for the economy due to created incentives to save rather than invest. The Austrian school counters this by arguing that prices drop in all stages of production, and that profit ratios consequently stay stable. According to the Austrian school of thought, deflation will lead to savings, which results in a drop in interest rates and subsequently new investments. Consequently, increased growth of the bitcoin economy, and the subsequent deflation of the monetary value of bitcoin, does not implicate an obstacle for the bitcoin economy according to the Austrian school. [17]

In its early years, bitcoin was highly inflationary. The growth rate is now moderately inflationary at an expected level of 4.5% in 2017, where after it is estimated to decline to 1.7% in 2021 and 0.8% in 2025. After this point, the growth rate will become increasingly negligible. A comparison of the supply of bitcoin to the monetary base of some major fiat currencies such as USD, JPY, CHF, EUR and GBP shows that bitcoin's growth rate dwarfs that of the fiat currencies. Due to the characteristics of bitcoin's pre-programmed finite supply, the tables are however expected to be turned within the next decade. By 2025, bitcoin's annual growth rate is expected to drop below that of all the world's major currencies and media of exchange – including gold. [17]

6 Conclusion

Below follows a short conclusion of each posed scientific question. The report ends with a broader discussion of the main objective of this report.

What technical prerequisites would a transition to a cryptocurrency require?
The technical prerequisites needed to maintain and use a Bitcoin payment system is the sufficient technical device, described in section 5.2, and an internet connection. The study showed that overall, Sweden has the needed technology to maintain a Bitcoin payment system. This includes fulfilling both the prerequisites for users and merchants, as well as the prerequisites for maintaining a functioning network. However, the study showed that a small minority of the Swedish population does not meet the technical prerequisites as this group lacks the equipment needed to participate. The study focused on Bitcoin but as the technology behind Bitcoin is advanced, the drawn conclusions should apply to any existing cryptocurrency of modern time.

What major opportunities and limitations would such a transition entail?
The study showed several opportunities as well as limitations with a transition to Bitcoin. Cheaper and more efficient cross border payments, open participation and protection of payer integrity are the most significant strengths of the protocol. Limitations such as scalability problems, high energy consumption and confirmation times of up to an hour, are the most serious limitations of the protocol.

The limitations require careful consideration, in order to avoid loss of functionality during a transition to cryptocurrency. One big limitation of Bitcoin is that the confirmation time of a transaction is not compatible with the modern way of conduction in-store commerce. Another factor that might inhibit the further growth of Bitcoin is the required energy consumption to maintain the network. Though it is difficult to make a quantitative comparison between Bitcoin and the traditional payment system in this area, Bitcoin do consume significant amounts of energy and the system is therefore likely to face resistance in this matter.

What safety concerns are associated with a transition to a cryptocurrency?
The study has exposed two main safety concerns, namely the centralization of the network and the underdeveloped user-system interaction. The security of Bitcoin relies on the decentralized network. Therefore, anything that could affect the decentralization negatively, centralizing the network to larger extent, is considered a safety concern. In addition, most Swedish inhabitants are custom to depending on the payment system without understanding its underlying technology. With Bitcoin however, such an approach could expose the user to financial and integrity risk, since a proper usage requires a certain level of understanding.

Could a cryptocurrency supply the functions of a traditional currency?
In theory, a cryptocurrency fulfils the functions of a currency but in reality, cryptocurrencies lack several features as of today. Though Bitcoin is the largest of the existing cryptocurrencies, it is not widely used for payments. The acceptance of Bitcoin is growing but it is rarely used by the masses, thus it is seldom used as a unit of account. However, bitcoin is divisible and more transportable than traditional currencies as well as it is easily stored. So far, the bitcoin

exchange rate has been very volatile, though it shows tendencies of maturing, which makes it inappropriate both as a store of value, and for transactional purposes. In order for it to work as a unit of account to express prices of goods and services, pricing of goods and services would have to be very dynamic.

Whether a cryptocurrency could serve as an official currency, viewed from a macroeconomic perspective, depends on what school of thought you belong to. Since the money supply of Bitcoin is fixed, using monetary policy for political purposes is not possible. However, some schools are of the belief that governmental interventions are not beneficial. Concluding, this is a matter of opinion.

Would a transition to a cryptocurrency, as national currency of Sweden, be possible and what would it imply for the Swedish society?
To conclude, and to answer the main objective of this report, it would be technically and theoretically possible to implement a cryptocurrency as a national currency of Sweden. However, it is our belief that it in practice would be difficult. A transition would have consequences on our way of conducting business today. While some areas would experience improvements of a transition, there are obstacles in other areas that must be resolved before a transition to cryptocurrency could be beneficial on a societal level. As a majority of the everyday commerce is in-store, a solution to the hour-long confirmation delays must be proposed in order for a cryptocurrency to be used as a mean of payment by the masses. It is however likely that bitcoin, and other cryptocurrencies, will continue to be used alongside traditional currencies, especially for cross-border payments and bank-to-bank transfers. This because the underlying technology of Bitcoin, and other cryptocurrencies, offers more time and cost efficient transaction processing than the traditional payment systems in these areas.

The technical infrastructure of Bitcoin creates interesting possibilities and we believe that Bitcoin will have a great effect on future payment systems. One possible application is a global payment system where the Bitcoin infrastructure is used for transporting value rather than making direct payments. However, bitcoin as a currency seems useful only to a limited extent as of today. This due to the volatility of the bitcoin exchange rate. Though it is maturing with decreasing fluctuations, we do not think that it will be stable enough to be implemented as a national currency. As bitcoin is a global currency, the exchange rate and its fluctuation are harder to both predict and control. Today bitcoin should rather be regarded as a speculative asset, and as an interesting possibility for the ones that lack trust in the traditional financial system.

Common for all cryptocurrencies is the need of improved usability. A national cryptocurrency must be easy to use and to protect from fraud attempts and misuse. Though cryptocurrencies provide open participation, they are only accessible for those with a technical understanding and the sufficient equipment. Before a transition could be initiated, a way to include those with limited technical knowledge must be found. A possible scenario is a national cryptocurrency based on a closed network constituting of trusted nodes. Such a scenario would require a clear owner of the blockchain for security enforcing and rule dictating. Some of the problems that Bitcoin struggles with would be eliminated by such a system. For example, the Proof-of-Work algorithm could be designed in a less energy consuming way and the currency might gain more acceptance by the masses due to the existence of a clear owner and issuer. Further on, a clear owner would implicate that the cryptocurrency would be covered by national laws which strengthens consumer protection and places less responsibility on the user. Though such a system contradicts the core values of Bitcoin, it might be a more realistic solution today.

In order to successfully implement, and gain acceptance for, a cryptocurrency we believe that a pronounced issuer must exist. This majorly due to practical reasons, since someone has to drive the development in order to gain acceptance from the masses. A possible and probable issuer is the Swedish Riksbank, who are currently investigating the possibility of issuing their own digital currency, e-krona. The interest and need of a cryptocurrency is established on the market, and numerous parties are currently investigating the possibilities that a cryptocurrency would imply. A nationally accepted cryptocurrency is therefore likely to emerge in the near future, but in what shape remains undetermined. Currently, the cryptocurrency market could be illustrated by a swim race - all participants stand ready at the starting pallets, afraid to dive in due to the risk of unexpected threats under the surface, but just as afraid of missing the start bell and getting behind.

References

[1] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available: https://bitcoin.org/bitcoin.pdf. Accessed: 2017-02-28.

[2] CoinMarketCap. Available: http://coinmarketcap.com/all/views/all/. Accessed: 2017-04-29

[3] Bitcoin.org. *FAQ*. Available: https://bitcoin.org/sv/faq. Accessed: 2017-04-14

[4] D. Tapscott and A. Tapscott. *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business and the World.* Brilliance Audio, Michigan, 2016

[5] VISA. *Småköp med kort fortsätter att öka i Sverige – svenskar de näst främsta kortanvändarna i Europa*. Available: https://www.visa.se/press/smaakoep-med-kort-fortsaetter-att-oeka-i-sverige-svenskar-de-naest-fraemsta-kortanvaendarna-i-europa-1234930?returnUrl=/press/listing?tag=kortanvändande. Accessed: 2017-02-16

[6] Riksbanken. *Sedel- och myntstatistik*. Available: http://www.riksbank.se/sv/Statistik/Sedel-och-myntstatistik/. Accessed: 2017-04-26

[7] PostNord. (2017, Feb). *E-Barometern helårsrapport 2016*. Available: http://www.hui.se/statistik-rapporter/index-och-barometrar/e-barometern. Accessed: 2017-03-01

[8] B. Segendorf. (2017, Mar, 20). Interview at the Riksbank, Stockholm

[9] OxfordDictionaries. *Currency*. Available: https://en.oxforddictionaries.com/definition/currency. Accessed: 2017-03-30

[10] N. Arvidsson. *Föreläsning 5: Paradigm och Pengar*. ME1312 Kunskapsbildning, Stockholm, 2016.

[11] Investopedia. *Digital Money*. Available: http://www.investopedia.com/terms/d/digital-money.asp. Accessed: 2017-03-28

[12] SiaPartners. (2015, Aug, 12). *What is virtual money?*. Available: http://en.finance.sia-partners.com/what-virtual-money. Accessed: 2017-03-28

[13] A.M. Antonopoulos. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media*, California, 2015

[14] Narayanan, J. Bonneau, E. Felten, A. Miller and S. Goldfeder. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, New Jersey*,* 2016

[15] Bitcoin.org. *Developer Guide*. Available: https://bitcoin.org/en/developer-guide. Accessed: 2017-02-28

[16] D. Ackefelt and A. Weidenblad. *Bitcoin i detaljhandeln*. Degree Project, Computer Science, Communication and Industrial Management, the Royal Institute of Technology, Stockholm, Sweden. 2016. Available: https://www.kth.se/social/files/56a0c6c8f2765474137ee8fe/ACKEFELT%20WEIDENBLADH%20KEX_SLUTGILTIG.pdf. Accessed: 2017-04-05

[17] S. Ammous. *Economics beyond Financial Intermediation: Digital Currencies' Possibilities for Growth, Poverty Alleviation, and International Development.* The Journal of Private Enterprise, Lebanese American University, 2015. Available: http://capitalism.columbia.edu/files/ccs/workingpage/2015/center_working_paper_ammous_economics_beyond_financial_intermediation_1.pdf. Accessed: 2017-04-05

[18] J. Donnelly. (2015, Nov, 18). *Bitcoin is growing up –an Infographic of the Ecosystem.* Available: https://bitcoinmagazine.com/articles/bitcoin-is-growing-up-an-infographic-of-the-bitcoin-ecosystem-1447865097/. Accessed: 2017-04-05

[19] Bitcoin.se. *Handlare.* Available: https://www.bitcoin.se/handlare/. Accessed: 2017-04-05

[20] XE. *Bitcoin to SEK.* Available: https://www.xe.com/currencycharts/?from=XBT&to=SEK&view=1Y. Accessed: 2017-04-28

[21] XE. *USD to SEK.* Available: https://www.xe.com/currencycharts/?from=USD&to=SEK&view=1Y. Accessed: 2017-04-28

[22] Langner. (2017, Feb, 12). *Is Bitcoin Growing Up?.* Available: https://www.bloomberg.com/gadfly/articles/2017-02-13/bitcoin-might-just-be-growing-up. Accessed: 2017-04-05

[23] IIS. (2016, Nov). *Svenskarna och internet 2016 - Undersökning om svenskarnas internetvanor.* (Version 1.1) Available: https://www.iis.se/docs/Svenskarna_och_internet_2016.pdf. Accessed: 2017-04-13

[24] Bitcoin.com. *Merchant Solutions.* Available: https://www.bitcoin.com/merchant-solutions Accessed: 2017-04-13

[25] Bitcoin Mining. *Bitcoin Mining Guide – Getting started with Bitcoin.* Available: https://www.bitcoinmining.com/getting-started/#sm. Accessed: 2017-04-13

[26] Bitcoin.org. *Full Node.* Available: https://bitcoin.org/en/full-node#minimum-requirements. Accessed: 2017-04-13

[27] P. Wuille. (2017, Jan, 10). *Segregated Witness and its Impact on Scalability @ SF Bitcoin Devs.* Available: https://segwit.org/pieter-wuille-segregated-witness-and-its-impact-on-scalability-sf-bitcoin-devs-7813eebcf3de. Accessed: 2017-04-17

[28] Faife. (2017, Jan, 5). *Will 2017 Bring an End to Bitcoin's Great Scaling Debate?.* Available: http://www.coindesk.com/2016-bitcoin-protocol-block-size-debate/. Accessed: 2017-04-17

[29] B. Segendorf. (2014, Oct, 1). *Vad är Bitcoin?.* Available: http://www.riksbank.se/sv/Press-och-publicerat/Nyheter/2014/Vad-ar-Bitcoin/. Accessed: 2017-04-21

[30] K. J. O'Dwyer and D. Malone. *Bitcoin Mining and its Energy Footprint.* Hamilton Institute, National University of Ireland Maynooth, Ireland. 2014. Available: http://eprints.maynoothuniversity.ie/6009/1/DM-Bitcoin.pdf. Accessed: 2017-04-17

[31] Blockchain.info. *Charts.* Available: https://blockchain.info/charts/. Accessed: 2017-04-06

[32] L. Parker. (2015, Jun, 16). *The Decline in Bitcoin Full Nodes.* Available: https://bravenewcoin.com/news/the-decline-in-bitcoins-full-nodes/. Accessed: 2017-04-06

[33] Investopedia. *Austrian School of Economics*. Available: http://www.investopedia.com/articles/economics/09/austrian-school-of-economics.asp. Accessed: 2017-04-15

[34] L. von Mises. *The Free Market and Its Enemies: Pseudo-Science, Socialism, and Inflation.* Foundation for Economics Educations, New York, 2004. Available: https://mises.org/system/tdf/Free_Market_and_Its_Enemies_The_2.pdf?file=1&type=document. Accessed: 2017-04-14

[35] ECB. (2012, Oct). *Virtual Currency Schemes – October 2012*. Available: http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf. Accessed: 2017-04-16

[36] Bitcoin.org. (2016, Mar, 19). *Podcast*: *Bitcoin Macroeconomics*. Available: https://www.bitcoin.com/podcast/bitcoin-macroeconomics. Accessed: 2017-04-17

[37] J. McWhinney. (2015, Apr, 5). *Why Governments are Afraid of Bitcoin.* Available: http://www.investopedia.com/articles/forex/042015/why-governments-are-afraid-bitcoin.asp. Accessed: 2017-04-17

[38] G. LeBlanc. *The effects of cryptocurrencies on the banking industry and monetary policy.* S.H. thesis, Economics Dep., Eastern Michigan University, Michigan, MI. 2016. Available: http://commons.emich.edu/cgi/viewcontent.cgi?article=1498&context=honors. Accessed: 2017-04-17

[39] E. Frost. (2016, Apr, 11). *The Impact of Bitcoin on Central Banks*. Available: https://internationalbanker.com/banking/impact-bitcoin-central-banks/. Accessed: 2017-04-17

[40] Riksbanken. *Inflation*. Available: http://www.riksbank.se/sv/Penningpolitik/Inflation/. Accessed: 2017-04-17